# RANK GAIN OF JACOBIAN VARIETIES OVER FINITE GALOIS EXTENSIONS

BO-HAE IM AND ERIK WALLACE

ABSTRACT. Let $K$ be a number field, and let $\mathcal{X} \to \mathbb{P}^1_K$ be a degree $p$-covering branched only at 0, 1, and $\infty$. If $K$ is a field containing a primitive $p$-th root of unity then the covering of $\mathbb{P}^1$ is Galois over $K$, and if $p$ is congruent to 1 mod 6, then there is an automorphism $\sigma$ of $\mathcal{X}$ which cyclically permutes the branch points. Under these assumptions, we show that the Jacobian varieties of both $\mathcal{X}$ and $\mathcal{X}/\langle\sigma\rangle$ gain rank over infinitely many linearly disjoint cyclic degree $p$-extensions of $K$. We also show the existence of an infinite family of elliptic curves whose $j$-invariants are parametrized by a modular function on $\Gamma_0(3)$ and that gain rank over infinitely many cyclic degree 3-extensions of $\mathbb{Q}$.

## 1. Introduction

The construction in this paper is inspired largely by a paper of Elkies on the Klein quartic [2], however we have been able to prove much more general results. The general setup is the following. Let $\mathcal{X}$ and $\mathcal{Y}$ be curves defined over a number field $K$, and suppose we have the following diagram

$$\begin{array}{ccc} & \mathcal{X} & \\ \swarrow & & \searrow \\ \mathcal{Y} & & \mathbb{P}^1_K \end{array} \tag{1}$$

where both maps are defined over $K$ and surjective, and the map $\mathcal{X} \to \mathbb{P}^1_K$ has degree $d > 1$. The strategy is to lift $K$-rational points $P$ of $\mathbb{P}^1_K$ to points $Q$ on $\mathcal{X}$, which in general will lie in an extension $L/K$. By Hilbert's irreducibility theorem it can be shown that $L/K$ will usually be a degree $d$ extension.

*Date*: December 12, 2016.

2010 *Mathematics Subject Classification.* Primary 14H40, 11G05 Secondary 12E25, 14H30.

Bo-Hae Im was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (NRF-2014R1A1A2053748).

We are especially interested in the case where $L/K$ is a Galois extension. If the map $\mathcal{X} \to \mathbb{P}^1_K$ is itself Galois (over $K$) with group $G$, then the degree $d$ extensions $L/K$ that are obtained from Hilbert's irreducibility theorem are also Galois with group isomorphic to $G$. But there are sometimes other ways of getting the extensions $L/K$ to be Galois without $\mathcal{X} \to \mathbb{P}^1_K$ being Galois itself as will be seen in the proof of Theorem 3.

As for the maps $\mathcal{X} \to \mathcal{Y}$, such maps can be obtained by taking quotients by a subgroup of the automorphism group of $\mathcal{X}$ or, in the case where $\mathcal{Y}$ is an elliptic curve and $\mathcal{X}$ is a suitable modular curve, they can be obtained from the modularity theorem. In a sense the case of the Klein quartic constitutes an example of both.

Once infinitely many points on $\mathcal{X}$ and $\mathcal{Y}$ have been produced, all lying in different degree $d$ extensions of $K$, they can then be used to construct corresponding points on the Jacobian varieties of $\mathcal{X}$ and $\mathcal{Y}$. Then by the generalization of a lemma of Silverman [9], it can be shown that the Jacobian varieties of $\mathcal{X}$ and $\mathcal{Y}$ each gain rank over infinitely many extensions $L/K$. If we are not concerned with the extensions $L/K$ being Galois, it is a relatively easy matter to show that the rank gains over infinitely many extensions $L/K$ for infinitely many different degrees as indicated by Proposition 5, but with the Galois condition added the problem becomes more difficult and essentially is related to the inverse Galois problem. In particular for elliptic curves it is not well understood whether an elliptic curve can gain rank over cyclic Galois extensions of a number field $K$, outside of some special cases. As the following theorem shows, the Klein quartic gives us rank gain for certain Elliptic curves over cyclic degree 7 extensions of $\mathbb{Q}(\zeta_7)$ where $\zeta_7$ is a primitive 7-th root of unity.

**Theorem 1.** *Let $p$ be a prime. Let $\mathcal{X}$ be a Riemann surface of genus $g > 1$ and let*

$$\varphi : \mathcal{X} \to \mathbb{P}^1_K$$

*be a degree $p$ Galois covering ramified only at 0, 1, and $\infty$. If $p \equiv 1 \mod 6$, then there is an automorphism $\sigma$ of $\mathcal{X}$ that cyclically permutes the points 0, 1, and $\infty$, and there are infinitely many linearly disjoint degree $p$-extensions $L/K$ over which the Jacobian variety of $\mathcal{Y} = \mathcal{X}/\langle\sigma\rangle$ gains rank.*

Note that for the covering $\varphi$ to be Galois over $K$, it is required to have $K$ to contain $\mathbb{Q}(\zeta_p)$ where $\zeta_p$ is a primitive $p$-th root of unity. Theorem 1 also has the following Corollary, which is an immediate consequence of the linear disjointness property.

**Corollary 2.** *Following the same notations as in Theorem 1, let $J_{\mathcal{X}}$ and $J_{\mathcal{Y}}$ be the Jacobian variety of $\mathcal{X}$ and $\mathcal{Y}$ respectively. Then $J_{\mathcal{X}}$ and $J_{\mathcal{Y}}$ have infinite rank over $K[p]^{ab}$, i.e. the maximal abelian extension $K[p]^{ab}$ of $K$ in the compositum $K[p]$ of all degree $p$-extensions.*

For $p = 7$, the curve $\mathcal{X}$ is the Klein quartic, which is also known to be the modular curve $X(7)$. It follows, that we not only have rank gain for the quotient curve, which Elkies [2] denotes by $E_k$, but also for any curve in the same isogeny class as $E_k$ and more generally for any elliptic curve with conductor 49. However, in all cases the degree 7 extensions $L/K$ obtained are only Galois extensions if $K$ contains $\mathbb{Q}(\zeta_7)$

From a slightly different perspective, it can be sometimes shown that the extensions $L/K$ in Proposition 4 are Galois even when the covering of $\mathbb{P}^1_K$ is not. In particular, we prove the following theorem for the genus 1-case.

**Theorem 3.** *There is an infinite family of elliptic curves over $\mathbb{Q}$ such that each member gains rank over infinitely many linearly disjoint cyclic degree 3-extensions of $\mathbb{Q}$.*

Here, the infiniteness of the family means that the $j$-invariants of elliptic curves in the family are distinct. Since an infinite family is obtained, one way of looking at the proof is in terms of a surface, the fibers of which are curves $\mathcal{X}$ with maps to $\mathbb{P}^1$. When viewed in this way, the curves $\mathcal{X}$ that occur in the construction can be seen to have genus 4. Recently, Professor Masanobu Kaneko pointed out to the first author that the $j$-invariant constructed in Theorem 3 is paramerized by a modular function on $\Gamma_0(3)$ whose more details are given at the end of the paper, hence it also can be viewed in terms as modularity just like the case of the Klein Quartic in Theorem 1.

It is worthwhile to compare Theorem 3 to Theorem C in [3] which shows that if an elliptic curve over $\mathbb{Q}$ has at least 6 rational points, then it gains rank over infinitely many cyclic degree 3-extensions of $\mathbb{Q}$. The proof of theorem 3 in this paper provides a family containing curves with rank zero over $\mathbb{Q}$ and rational torsion isomorphic to $\mathbb{Z}/3\mathbb{Z}$, hence Theorem C [3] does not apply to those curves. On the other hand all curves in the family found in Theorem 3 have non-trivial rational 3-torsion, hence Theorem C in [3] applies to any Elliptic curve with positive rank over $\mathbb{Q}$ and trivial torsion, but none of those curves are included in our proof of Theorem 3. As a consequence not only are the methods used to obtain the theorems completely, but there are elliptic curves that are known by one of them to grain rank, but not by the other.

The next proposition provides the basic machinery used to prove 1 and 3 above.

**Proposition 4.** *Let $\mathcal{X}$ be a smooth irreducible curve of genus $g > 1$, defined over a number field $K$, and let*

$$\mathcal{X} \to \mathbb{P}^1_K$$

*be a covering map of degree $d > 1$. Then there exist infinitely many linearly disjoint extensions $L/K$ of degree $d$ over which the Jacobian variety of $\mathcal{X}$ gains rank. Additionally, if the covering is Galois with group $G$, than there are infinitely many such extensions which are Galois with group $G$.*

It has already been pointed out that maps can be obtained from $\mathcal{X} \to \mathcal{Y}$ by taking a quotient, or in the case where $\mathcal{X}$ is a modular curve maps can be obtained to elliptic curves $E$ by the modularity theorem. But there is another option: given a morphism from the Jacobian variety of $\mathcal{X}$ to another abelian variety $A$, all results can be extended to the abelian variety. Also if we are not concerned with the extensions $L/K$ being Galois, then it is relatively easy to obtain the following generalization of Theorem 1 in [6]:

**Proposition 5.** *Let $\mathcal{X}$ be a smooth irreducible curve of genus $g > 1$, defined over a number field $K$. Then there is a constant $N$ depending on $\mathcal{X}$ but not on $K$ such that for every positive integer $d \geq N$, there exist infinitely many linearly disjoint degree $d$-extensions $L/K$ over which the Jacobian variety of $\mathcal{X}$ gains rank.*

It is important to note that this generalization improves on two details:

(1) For Theorem 1 in [6], it is assumed that the curve is bi-rationally equivalent over $K$ to a plane curve of the form $f(x) = g(y)$, where the degrees of $f$ and $g$ are co-prime. This assumption excludes hyper-elliptic curves $y^2 = f(x)$ for which the degree of $f$ is even, and it excludes curves $f(x, y) = 0$ for which the variables cannot be separated. By contrast the proof of Proposition 5 is done generally enough so as to cover these cases as well.
(2) For Theorem 1 in [6] the degree is assumed to be prime $p$, whereas in Proposition 5 the degree may be composite.

The constant $N$ is explicit as it is shown in its proof. Even with these improvements however, the biggest shortcoming of Proposition 5 is the fact that the extensions obtained are generally not Galois, and an

analogous statement of the result for Galois coverings remains an open problem.

**Acknowledgments.** This project began as a collaboration with Neeraj Kashyap who made some key contributions to the construction in the early stages, but later became otherwise occupied. The authors would also like to thank Taylor Dupuy for suggesting the work of Ledet, and Michael Larsen for suggesting generalizations to our results, which have been incorporated in the current version. The authors would also like to thank Professor Masanobu Kaneko for making the observation about eta functions as in Remark 12.

## 2. Proofs

To prove Proposition 4 and Theorem 1 we will need the following lemma, originally proven by Silverman in the genus 1 case [9]. We include a self-contained proof cause due to the lack of its presence in the literature.

**Lemma 6.** *Let $K$ be a number field, and $A$ be an abelian variety defined over $K$. Then for every positive integer $d$, we have*

$$\left| \bigcup_{[L:\mathbb{Q}]\leq d} A(L)_{tor} \right| < \infty,$$

*where $A(L)_{tor}$ denotes the set of torsion points of $A$ that are $L$-rational.*

The general proof is similar, but it appears nowhere in print and so we briefly give the proof here.

*Proof.* Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be two prime ideals of $K$ with distinct residue characteristics $p_1$ and $p_2$ respectively, at which $A$ has good reduction. Let $L/K$ be an extension such that $[L:K] \leq d$, and let $\mathfrak{P}_1$ and $\mathfrak{P}_2$ be two primes above $\mathfrak{p}_1$ and $\mathfrak{p}_2$ respectively. Then there exists an injective map

$$A_m(L) \to A_m(\mathcal{O}_L/\mathfrak{P}_i)$$

where $A_m$ denotes the $m$-torsion of $A$ (see for example [1, Ch. 7, Proposition 3]). By the Lang-Weil bound we have

$$|A_m(\mathcal{O}_L/\mathfrak{P}_i)| \ll N_{L/\mathbb{Q}}\mathfrak{P}_i \ll \left(N_{K/\mathbb{Q}}\mathfrak{p}_i\right)^d$$

where the implied constants depend only on $A$. For an arbitrary positive integer $m$, if $m_i$ denotes the largest factor of $m$ not divisible by $p_i$,

then by the structure theorem of finite abelian groups we have

$$|A_m(L)| \leq |A_{m_1}(L)| \cdot |A_{m_2}(L)| \ll \left(N_{K/\mathbb{Q}}\mathfrak{p}_1\mathfrak{p}_2\right)^d.$$

Since the right hand side of this estimate does not depend on $m$ or $L$, and since number of options for $\mathcal{O}_L/\mathfrak{P}_i$ is finite (up to isomorphism), this completes the proof. □

We will also need the following lemma which is essentially a direct application of Hilbert's irreducibility theorem.

**Lemma 7.** *Let $\mathcal{X}$ be a smooth irreducible curve of genus $g > 0$ defined over a number field $K$, and let*

$$\mathcal{X} \to \mathbb{P}^1_K$$

*be a covering map of degree $d > 1$. Then there exist infinitely many linearly disjoint extensions $L/K$ of degree $d$ such that $\mathcal{X}$ has an $L$-rational point. Additionally, if the covering is Galois with group $G$, then there are infinitely many such extensions $L/K$ which are Galois with group $G$.*

*Proof.* In the Galois case this is [8, Corollary 3.3.4]. For the general case, let $\mathcal{Y}$ be the Galois closure of $\mathcal{X}$ such that the covering

$$\pi : \mathcal{Y} \to \mathbb{P}^1$$

has group $G$, and let $H_0 \leq G$ be a subgroup such that $\mathcal{Y}/H_0 \cong \mathcal{X}$. If $L/K$ is an arbitrary finite extension, then

$$A_L = \bigcup_{H<G} \pi_H(\mathcal{X}/H)(L)$$

is thin with respect to $L$, where the union is over proper subgroups $H$ of $G$, and $\pi_H$ is the natural morphism to $\mathbb{P}^1$ induced by taking the quotient by $H$. This set has the property that if $P \notin A_L$ then $P$ lifts to a point $Q \in \mathcal{X}(M)$ where $M/L$ is a degree $d$-extension (the proof is analogous to that of [8, Prop. 3.3.1]).

By [8, Prop. 3.2.1] the set $A := A_L \cap K$ is thin with respect to $K$, so by applying the above argument to $P \in \mathbb{P}^1(K)\backslash A$ we obtain the result by induction by taking $L$ to be the compositum of all previously obtained degree $d$-extensions. □

**Remark 8.** *In the special case of a Galois covering ramified only at 0, 1 and $\infty$ and of degree $p$, where $p$ is an odd prime, we obtain an equation*

$$y^p = x^r(x-1)^s$$

*as an affine model, where $r$, $s$ and $r+s$ are relatively prime to $p$. When $K = \mathbb{Q}$ it can be actually shown that 0, 1, and $\infty$ are the only*

*exceptions. This is done as follows. Take* $x = \frac{a}{b}$*, where* $a, b$ *are rational integers. By the pairwise relative primality of* $a, b, a-b$*, and unique factorization, it can be shown that* $a, b, a-b$ *each must be a pth power, say* $A^p, B^p, C^p$ *in* $\mathbb{Z}$ *respectively. Then we must have an integer solution to*

$$A^p = B^p + C^p,$$

*by Fermat's Last Theorem we know that the only solutions are trivial, and the trivial solutions correspond to the points* $0$*,* $1$*, and* $\infty$*.*

**Proposition 9.** *Let* $\mathcal{X}$ *be a smooth irreducible curve. Suppose there exist a finite subgroup* $G \subseteq \mathrm{Aut}(\mathcal{X})$ *and a nontrivial abelian variety* $\mathcal{A}$ *satisfying the following conditions:*

1. *there exists a morphism* $f : \mathcal{X} \to \mathcal{A}$*, and*
2. *there exists a homomorphism* $\phi : G \to \mathrm{Aut}(\mathcal{A})$ *such that* $f(\sigma(x)) - f(x) = \phi(\sigma)$ *for all* $\sigma \in G$ *and for all* $x \in \mathcal{X}$*.*

*Then if* $f(\mathcal{X})$ *generates* $\mathcal{A}$*, then* $\dim(\mathcal{A}) \leq g(\mathcal{X}/G)$*, where* $g(\mathcal{X}/G)$ *is the genus of* $\mathcal{X}/G$*.*

*Proof.* We may take a pair $(\mathcal{X}, G)$ with $|G|$ minimal among all such pairs satisfying conditions (1) and (2). Let $H$ be a subgroup of $G$ generated by all elements $h \in G$ satisfying that there exists $x \in \mathcal{X}$ such that $h(x) = x$. Then $H$ is a normal subgroup of $G$. Indeed, for $h \in H$ and $\sigma \in G$, there exists $x \in \mathcal{X}$ such that $h(x) = x$ and so for $\sigma^{-1}(x) \in \mathcal{X}$, $(\sigma^{-1}h\sigma)(\sigma^{-1}(x)) = \sigma^{-1}(h(x)) = \sigma^{-1}(x)$.

Condition (2) implies that for every $h \in H$, $\phi(h) = 0$, in other words $f(h(x)) = f(x)$ for all $x \in \mathcal{X}$. Hence $f$ factors through $\mathcal{X}/H$, giving us a quotient curve $\mathcal{X}/H$ over $\mathbb{P}^1$ which maps to $\mathcal{A}$, and so if we replace $(\mathcal{X}, G)$ by $(\mathcal{X}/H, G/H)$ both conditions (1) and (2) are still satisfied. By the minimality of $|G|$, $H$ must be trivial. So each $\sigma \in G$ has no fixed point on $\mathcal{X}$. Hence we may assume that $G$ acts freely on $\mathcal{X}$.

We define a map $F : J(\mathcal{X}) \to \mathcal{A}$ as follows; for $x_i, y_j \in \mathcal{X}$,

$$F\left(\sum_{i=1}^{n}[x_i] - \sum_{i=1}^{n}[y_i]\right) = \sum_{i=1}^{n} f(x_i) - \sum_{i=1}^{n} f(y_i).$$

The map $F$ is well defined because every morphism from a rational curve to an abelian variety is constant, hence linearly equivalent divisors map to the same element of $\mathcal{A}$, and it is surjective because of the assumption that $f(\mathcal{X})$ generates $\mathcal{A}$. Moreover, condition (2) implies that for $\sigma \in G$,

$$F\left(\sum_{i=1}^{n}[\sigma(x_i)] - \sum_{i=1}^{n}[\sigma(y_i)]\right) = F\left(\sum_{i=1}^{n}[x_i] - \sum_{i=1}^{n}[y_i]\right),$$

so $F$ is $G$-equivariant. Therefore, by identifying $J(\mathcal{X})(\mathbb{C})$ with the quotient $\mathrm{H}_1(\mathcal{X}(\mathbb{C}),\mathbb{R})/\mathrm{H}_1(\mathcal{X}(\mathbb{C}),\mathbb{Z})$, there exists a surjective morphism from $\mathrm{H}_1(\mathcal{X}(\mathbb{C}),\mathbb{R})$ onto the Lie algebra $\mathrm{Lie}(\mathcal{A})$ of $\mathcal{A}$, and this is $G$-equivariant by [7, Ch. 6]. Hence we have $\dim(\mathcal{A}) \leq \dim(\mathrm{H}_1(\mathcal{X}(\mathbb{C}),\mathbb{R})) = \dim(\mathrm{H}_1(\mathcal{X}/\mathcal{G}(\mathbb{C}),\mathbb{R})) = g(\mathcal{X}/G)$. □

Now we are ready to prove Proposition 4.

*Proof of Proposition 4.* Since $\mathcal{X}$ is a cover of $\mathbb{P}^1_K$ over $K$, there exist infinitely many degree $d$ divisors $D_Q$ on $\mathcal{X}$ that are the preimages of $K$-rational points $Q$ of $\mathbb{P}^1$ and are defined over $K$.

Fix one of $D_Q$ say, $D$. Then pick any point $P_Q$ on $\mathcal{X}$ that lies in the preimage of $Q$ (i.e., belongs to the support of $D_Q$) and consider the degree zero divisor $d[P_Q] - D$ and (its linear equivalence class) the corresponding point $\widetilde{P_Q}$ of the Jacobian variety $J(\mathcal{X})$ of $\mathcal{X}$, which defines a $K$-rational non-constant morphism $f$ from $\mathcal{X}$ to $J(\mathcal{X})$, i.e. $f(P) := d[P] - D$.

Now by varying $Q$ in $\mathbb{P}^1_K$ or by Lemma 7 there are infinitely many points $\{P_i\}_i$ on $\mathcal{X}$ such that $P_i \in \mathcal{X}(L_i) \setminus \mathcal{X}(K)$, where $L_i$ are linearly disjoint degree $d$-extensions of $K$. Let

$$D_i = d[P_i] - D$$

denote the corresponding divisor in $J(\mathcal{X})$. Each divisor $D_i$ gives us a point on $J(\mathcal{X})$ defined over each degree $d$-extension $L_i$ of $K$ via the $K$-rational map $f$. By Lemma 6, all but finitely many $D_i$ are non-torsion points of $J(\mathcal{X})$.

Now we claim that for infinitely many $i$, $D_i$ are not defined over $K$. For the Galois closure $\mathcal{Y}$ of $\mathcal{X}$ which is a Galois cover of $\mathbb{P}^1_K$, let $G_0$ be a group isomorphic to each Galois closure of $L_i$ over $K$. Let $\pi : \mathcal{Y} \to \mathcal{X}$ and $H \subseteq G_0$ such that $\mathcal{Y}/H = \mathcal{X}$. Let $G := \{\sigma \in G_0 : f(\pi(\sigma(y))) - f(\pi(y))$ is a constant for all $y \in \mathcal{Y}\}$. Then $G$ is normal in $G_0$ (similarly as we have shown in the proof of Proposition 9) and $H \subseteq G$. Let $\mathcal{X}' := \mathcal{Y}/G$. Then we have a non-constant map $g$ from $\mathcal{X}$ to $\mathcal{X}'$. Since the genus $g(\mathcal{X})$ of $\mathcal{X}$ is greater than 1, we have that $g(\mathcal{X}) > g(\mathcal{X}')$ unless $G = H$, and $g(\mathcal{X}) = g(\mathcal{X}')$ if and only if $G = H$ (i.e. $g$ is an isomorphism). On the other hand, since $f(\mathcal{Y})$ generates $J(\mathcal{X})$ via $f \circ \pi$, Proposition 9 implies that $g(\mathcal{X}) \leq g(\mathcal{Y}/G) = g(\mathcal{X}')$. Therefore, we conclude that $G = H$, i.e. $\mathcal{X} = \mathcal{Y}/G$. This implies that for any element $\tau$ in $G_0 \backslash G$, $f(\tau(x)) - f(x)$ is not constant for all $x \in \mathcal{X}$. Hence there are infinitely many $i$ such that $f(x_i) = D_i$ are not defined over $K$.

Hence there are infinitely many non-torsion points $D_i \in J(\mathcal{X})(L_i) \setminus J(\mathcal{X})(K)$. Moreover, by Lemma 6, there are infinitely many $i$ such that $\sigma(D_i) - D_i$ are not torsion for all $\sigma \in G_0$. In order to show that they are linearly independent, if

$$n_1 D_1 + n_2 D_2 + \cdots n_k D_k = O, \text{for some integers } n_i, \tag{2}$$

for each $i$, there exists $\sigma_i \in \mathrm{Gal}(L_1 L_2 \cdots L_k / K)$ such that $\sigma_i(D_i) \neq D_i$ but $\sigma_i(D_j) = D_j$ for all $j \neq i$ by the linear disjointness of $L_i$. Then by applying $\sigma_i$ to Eq. (2) and subtracting one from another, we get $n_i(\sigma(D_i) - D_i) = O$, which leads a contradiction. Hence the rank of $J(\mathcal{X})$ gains over each $L_i$. □

*Proof of Proposition 5.* Every curve $\mathcal{X}$ is bi-rationally equivalent to a plane curve, allowing for singularities. Irreducibility, however, is preserved. Let $\mathcal{C}$ be such a plane curve, and suppose it is given by a homogeneous equation

$$F(X_0 : X_1 : X_2) = 0$$

where we define $n = \deg F$. We now make a change of variables as follows. Let $L/K$ be a finite extension such that $\mathcal{C}$ has a non-singular point $P_1$ defined over $L$. Then choose a second point have $P_2$, not lying on $\mathcal{C}$ such that the directional derivative

$$\nabla_{\overrightarrow{P_1 P_2}} F(P_1)$$

does not vanish (i.e. $P_2$ does not lie on the tangent of $\mathcal{C}$ at $P_1$). The points $P_1$ and $P_2$ together define a line in $\mathbb{P}^2$; let $P_0$ be a point not on this line. Finally if $P_i = (a_{i0} : a_{i1} : a_{i2})$ are $X_0, X_1, X_2$-coordinates, then

$$X_i = a_{i0} U_0 + a_{i1} U_1 + a_{i2} U_2$$

defines a change of variables, such that $F(U_0 : U_1 : U_2)$ has the following properties:

(1) The coefficient of $U_1^n$-term vanishes,
(2) The coefficient of $U_1^{n-1} U_2$-term does not vanish.

In the new coordinates, $F$ is defined over $L$, however there is enough freedom to the choice of $P_2$ and $P_0$ so that if $a_{1j} \in L \setminus K$, then $a_{2j}$ and $a_{0j}$ can be chosen such that

$$\frac{a_{2j}}{a_{1j}}, \frac{a_{0j}}{a_{1j}} \in K.$$

We can then re-scale by the substitution $V_j = a_{1j} U_j$. On the other hand if $a_{1j} \in K$ then we simply take $a_{2j}, a_{0j} \in K$ and $V_j = U_j$. The combined effect is that we obtain a projective linear transformation of $\mathbb{P}^2$ defined over $K$, such that $F(V_0 : V_1 : V_2)$ has the same two

properties as $F(U_0 : U_1 : U_2)$ above. Dividing $F(V_0 : V_1 : V_2)$ by $V_0^n$ and making the substitution

$$v_1 = \frac{V_1}{V_0} \quad \text{and} \quad v_2 = \frac{V_2}{V_0}$$

gives us an equation $f(v_1, v_2) = 0$ defining $\mathcal{C}$. By construction the polynomial $f$ is defined over $K$ and irreducible. We now construct an auxiliary curve $\mathcal{C}_1$ from $f$ by the substitution.

$$v_1 = s + t^{k_1} \quad \text{and} \quad v_2 = b + t^{k_2}$$

for suitable $k_1, k_2 \in \mathbb{Z}^+$ and $b \in K$. The polynomial $g(s,t)$ defining $\mathcal{C}_1$ must be designed to be irreducible and have degree $d = k_1(n-1) + k_2$. Since $f$ is irreducible, by Hilbert's irreducibility theorem there exists $b \in K$ such that $f(v_1, b)$ is irreducible. Under the substitution we have

$$f(s, b) = g(s, 0),$$

and so $g(s,t)$ must be irreducible with this choice of $b$.

To obtain the desired degree, we plot the exponents $(n_i, n_j)$ of all non-vanishing terms $c_{ij} v_i^{n_i} v_j^{n_j}$ of $f$ in a plane. Now consider the region $R$ formed by the convex hull of these points. The two properties of mentioned above imply that $(n-1, 1)$ is a corner point of $R$, hence by the graphical method of solving a linear programming problem

$$k_1 n_1 + k_2 n_2$$

will attain its maximum value for the region $R$ uniquely at the point $(n-1, 1)$ if the slope of the line $k_1 n_1 + k_2 n_2 = 0$ is less than $-1$. Since the slope is $-k_1/k_2$, this means we need $k_1 > k_2$.

Now we need to determine what values of $d = k_1(n-1) + k_2$ are possible, with positive integers $k_1, k_2$ satisfying $k_1 > k_2$. If we increase $k_1$ by 1, the value of $d$ goes up $n-1$, and this gap can be filled in by $k_2$ if and only if $k_2$ is allowed to range over $n-1$ consecutive integers. This makes $n$ the minimum value for $k_1$ and hence we obtain:

$$N = n(n-1) + 1.$$

Applying Proposition 4 to the curve $\mathcal{C}_1$ where the covering of $\mathbb{P}^1$ is obtained by taking the $s$-coordinate, completes the proof. □

**Remark 10.** *In some cases it is possible to get a better value for $N$. For example, for certain curves we may be allowed to take $k_1 = k_2$. The maximum value may no longer be uniquely obtained at $(n-1, 1)$, but if the cancellation of the highest degree terms of $f$ does not occur, this maximum may still be the degree. In that case we are allowed to take $N = (n-1)^2 + 1$.*

*Also, if we are only interested in prime degree, and pay attention to the prime gaps, we can do better. For example, in the case of the corollary for elliptic curves, we have $n = 3$ giving us $N = 7$ at least. But 5 is also obtained by $k_1 = 2$ and $k_2 = 1$, and we can get 2 and 3 by applying Proposition 4 directly to the elliptic curve.*

Next, we consider the special case of a degree $p$-Galois covering that is ramified at 0, 1, and $\infty$. By taking $p = 7$, this includes the Klein quartic as a special case. There are a couple of interesting things to note about this case. The first is that when the construction is done over $K/\mathbb{Q}(\zeta)$, where $\zeta$ is a primitive 7-th root of unity, the extensions $L/K$ are cyclic Galois extensions. The second is that by Remark 8, for $K = \mathbb{Q}$ or $\mathbb{Q}(\zeta)$ the only $K$-rational points which don't lift to a point lying in a degree 7 extension are 0, 1, and $\infty$. For $K = \mathbb{Q}(\zeta)$ we use Hilbert's correction of Kummer's proof in the case of regular primes (see [4]).

*Proof of Proposition 1.* First we investigate the situation with an automorphism of $\mathcal{X}$ that cyclically permutes the points 0, 1, and $\infty$. Given loops $\gamma_0, \gamma_1, \gamma_\infty$, about the points 0, 1, $\infty$ respectively each with the same winding number $Np$ for some positive integer $N$, these loops will lift to complete loops in $\mathcal{X}$ with winding numbers $w_0$, $w_1$, $w_\infty$, which must satisfy

$$w_0 + w_1 + w_\infty \equiv 0 \mod p. \tag{3}$$

Now suppose that $\mathcal{X}$ has an automorphism that cyclically permutes the points 0, 1, and infinity. If we take $N$ to be a common multiple of the minimal values for $w_0$, $w_1$, $w_\infty$, then the lifts of $\gamma_0, \gamma_1, \gamma_\infty$ will remain complete loops under the automorphism. Furthermore, the automorphism causes $w_0$, $w_1$, and $w_\infty$ to be multiples of each other mod $p$, say

$$w_1 \equiv c_0 w_0 \bmod p, \quad w_\infty \equiv c_1 w_1 \bmod p, \quad w_0 \equiv c_2 w_\infty \bmod p$$

for some integers $c_0, c_1, c_2$, and in fact it can be shown that $c_0$, $c_1$, and $c_2$ must be the same mod $p$, hence (3) reduces to

$$1 + n + n^2 \equiv 0 \mod p \tag{4}$$

for some positive integer $n$ which can be taken less than $p$. In terms of equations, this means we have the affine model defined by

$$y^p = x^n(x - 1). \tag{5}$$

For $p = 7$ this agrees with [2, equation 2.2] up to a change of variables. From the quadratic reciprocity we see that (4) has a solution when $p = 3$ or $p \equiv 1 \mod 6$. However, in the case $p = 3$, equation (5) defines

an elliptic curve, and the quotient by the cyclic permutation gives us an isogeny, so in this case we do not really get anything beyond what Proposition 4 already states.

Whenever a solution to (4) exists, we can show that $\mathcal{X}$ has an automorphism that cyclically permutes 0, 1, and $\infty$, in the following way. We do this by considering an auxiliary curve $\mathcal{Y}$, having a map to $\mathcal{X}$, and actually, for certain values of $p$, the curve $\mathcal{Y}$ is actually a non-singular model for $\mathcal{X}$. In particular we define $\mathcal{Y}$ as follows: for a given integer $m \geq 0$,

$$X^m Y + Y^m Z + Z^m X = 0. \tag{6}$$

It is non-singular and has an automorphism that cyclically permutes the points

$$(1:0:0),\ (0:1:0),\ (0:0:1).$$

For convenience, let $S := \{(1:0:0),\ (0:1:0),\ (0:0:1)\}$. The fixed points of this automorphism are

$$(\rho : \rho^2 : 1) \quad \text{and} \quad (\rho^2 : \rho : 1) \tag{7}$$

where $\rho$ is a primitive cube root of unity. These do not always lie on the curve, and as we shall see this is the difference between the cases $p = 3$ and $p \equiv 1 \mod 6$. Following Elkies [2], we set up a map from $\mathcal{Y}\backslash S$ to the line $a + b + c = 0$ in $\mathbb{P}^2$ in the obvious way:

$$\psi : (X : Y : Z) \mapsto (X^m Y : Y^m Z : Z^m X).$$

This map can be extended to all of $\mathcal{Y}$ by defining

$$\varphi : (1:0:0) \mapsto (1:0:-1),$$
$$\varphi : (0:1:0) \mapsto (-1:1:0),$$
$$\varphi : (0:0:1) \mapsto (0:-1:1),$$

and it is easy to check that when $\psi$ is extended in this way, it remains continuous. If $(a : b : c)$ is a point in the image of this map $\varphi$, it is easy to verify that

$$\left(\frac{Y}{Z}\right)^{m^2-m+1} = \frac{ab^{m-1}}{c^m}.$$

By making the substitution $u = -\frac{b}{c}$ and $v = (-1)^{m-1}Y/Z$, this give us

$$v^{m^2-m+1} = u^{m-1}(u-1). \tag{8}$$

Equation (5) can be obtained from this by the additional substitutions $x = u$, $y = v^{(m^2-m+1)/p}$ and $n = m - 1$, which essentially amounts to taking a quotient.

Now it be calculated that the automorphism of $\mathcal{Y}$ that cyclically permutes the variables $X, Y, Z$ passes to an automorphism of $\mathcal{X}$ permuting

$0, 1, \infty$, and when $p \equiv 1 \mod 6$ the two fixed points in (7) give us two fixed points in the model (5) with $x$ and $y$ coordinates in the form $\pm\rho^i$ for $i = 1, 2$. For $p = 3$, they do not lie on the curve. Hence by applying the Riemann-Hurwitz formula with this ramification data, we find that the genus of the quotient is

$$g = \begin{cases} \frac{p-1}{6} & \text{if } p \equiv 1 \mod 6 \\ 1 & \text{if } p = 3. \end{cases}$$

Any $K$-rational point on $\mathcal{X}$ maps to a $K$-rational point on the quotient, so the rest of the argument is the same as the proof of Proposition 4. □

To prove Theorem 3 we need the concept of a generic polynomial. The book [5] by Jensen, Ledet, and Yui gives a good introduction to the subject. In particular, we will use following lemma to construct a generic polynomial for a cyclic degree 3-extension of $\mathbb{Q}$.

**Lemma 11.** *Let $f$ be a cubic polynomial that is irreducible over a number field $K$, and let $d(f)$ be its discriminant. Then*

$$\mathrm{Gal}(f/K) \simeq \begin{cases} S_3 & \text{if } d(f) \notin (K^\times)^2, \\ C_3 & \text{if } d(f) \in (K^\times)^2, \end{cases}$$

*where $S_3$ is the symmetric group on 3 letters and $C_3$ is the cyclic group of order 3.*

The point is that if we allow the coefficients of $f$ to have parameters, and we use Hilbert's irreducibility theorem to obtain values of those parameters such that $f$ remains irreducible over the ground field, then this theorem allows the Galois group to be determined. The conditions for this turn out to be much weaker than those for a covering of $\mathbb{P}^1$ to be Galois, and this is what enables us to prove Theorem 3.

*Proof of Theorem 3.* Consider the polynomial

$$f(x, t) = x^3 + (a_4 - a_1 t)x + (a_6 - a_3 t - t^2) \tag{9}$$

where $a_4, a_1, a_6, a_3 \in \mathbb{Q}$ are to be determined. For convenience, we assume that

$$a_3 = a_1 \frac{a_6}{a_4} - \frac{a_4}{a_1},$$

so that $a_6 - a_3 t - t^2$ contains $a_4 - a_1 t$ as a factor. Then the discriminant is

$$d(f) = \left( -4(a_4 - a_1 t) - 27 \left( \frac{a_6}{a_4} + \frac{t}{a_1} \right)^2 \right) (a_4 - a_1 t)^2 \tag{10}$$

Our strategy is to use the Diophantine methods to find the values of $t$ making $d(f)$ a square in $\mathbb{Q}$. While $f(x, t)$ gives us a covering, it does not

give us a generic polynomial with $C_3$ as the Galois group. Effectively the Diophantine approach replaces $t$ with an auxiliary variable $s$ such that $f(x,s)$ becomes a generic polynomial with $C_3$ as the Galois group.

By completing the square, the first factor in equation (10) satisfies that

$$\begin{aligned}-4(a_4 - a_1 t) - 27\Big(\frac{a_6}{a_4} + \frac{t}{a_1}\Big)^2 \\ = 4\left(\frac{a_1^4}{27} - a_1^2\frac{a_6}{a_4} - a_4\right) - 27\left(\frac{t}{a_1} + \frac{a_6}{a_4} - \frac{2a_1^2}{27}\right)^2.\end{aligned}$$

If we set the first term $4\left(\frac{a_1^4}{27} - a_1^2\frac{a_6}{a_4} - a_4\right)$ equal to 1, this reduces the number of free variables by 1 giving us

$$a_6 = \frac{a_4 a_1^2}{27} - \frac{a_4}{4a_1^2} - \frac{a_4^2}{a_1^2}.$$

The Diophantine equation

$$1 = u^2 + 3v^2$$

can be solved in the same way as the Pythagorean case. In particular we have

$$u = \frac{1-3s^2}{1+3s^2} \quad \text{and} \quad v = 3\left(\frac{t}{a_1} + \frac{a_6}{a_4} - \frac{2a_1^2}{27}\right) = \frac{2s}{1+3s^2}.$$

This parameterization allows $t$ to be replaced by a rational expression in $s$ such that the discriminant of $f(x,s)$ is

$$d(f) = u^2(a_4 - a_1 t)^2.$$

Applying Hilbert's irreducibility theorem gives us infinitely many values $s \in \mathbb{Q}$ such that $f(x,s)$ is irreducible over $\mathbb{Q}$, and by lemma 11, the roots of any such polynomial will generate a cyclic degree 3 extension of $\mathbb{Q}$. In terms of the elliptic curve $E$ defined by $f(x,t) = 0$, where $f(x,t)$ is given in (9), this means that the specific $t$ values we get from rational $s$ values give us points $(x,t)$ on $E$ where the $x$-coordinate lies in a cyclic degree 3-extension $L/\mathbb{Q}$. Since changing the value of $s$ gives us infinitely many different values of $t$, we obtain infinitely many cyclic degree 3-extensions $L/\mathbb{Q}$ over which $E$ gains rank. The linear disjointness also follows in the same way as in the proof of Lemma 7.

As for which elliptic curves this occurs for, it would seem that the variables $a_1$ and $a_4$ remain undetermined. However, when computing the $j$-invariant, the variable $a_4$ cancels out and we are left with an

expression depending only on $a_1$, namely

$$j = 256\frac{(a_1^4+54)^3 a_1^4}{(4a_1^4-27)^3}. \tag{11}$$

□

**Remark 12.** *Recall that the function $f$ defined by*

$$f(z) = \Big(\frac{\eta(z)}{\eta(3z)}\Big)^2 = q^{-1} + 15 + 54q - 76q^2 - 243q^3 + 1188q^4 - \cdots$$

*is a modular function on $\Gamma_0(3)$. And the $j$-invariant given in* (11) *can be paramatrized as follows: Letting $a_1^4 = \frac{f}{4}$,*

$$j = \frac{f(f+216)^3}{(f-27)^3}.$$

*We deeply thank Professor Masanobu Kaneko for letting us this observation.*

## References


[1] Bosch, Siegfried and Lütkebohmert, Werner and Raynaud, Michel, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], Vol. 21, Springer-Verlag, Berlin, 1990.

[2] Elkies, Noam D., *T*he Klein quartic in number theory, The eightfold way, Math. Sci. Res. Inst. Publ., Vol. 35 (1999), Cambridge Univ. Press, Cambridge, 51–101.

[3] Fearnley, Jack and Kisilevsky, Hershy and Kuwata, Masato, *Vanishing and non-vanishing Dirichlet twists of L-functions of elliptic curves*, J. Lond. Math. Soc. (2), 86(2) (2012), 539–557.

[4] Grosswald, Emil, *Topics from the theory of numbers*, Modern Birkhäuser Classics, Reprint of the 1984 second edition [MR0807527], Birkhäuser Boston, Inc., Boston, MA, 2009.

[5] Jensen, Christian U. and Ledet, Arne and Yui, Noriko, *Generic polynomials*, Mathematical Sciences Research Institute Publications, Constructive aspects of the inverse Galois problem, Vol. 45, Cambridge University Press, Cambridge, 2002.

[6] Mendes da Costa, Dave, *On ranks of Jacobian varieties in prime degree extensions*, Acta Arith., Vol. 161, no.3 (2013), 241–248.

[7] Serre, Jean-Pierre, *Local fields*,

[8] Serre, Jean-Pierre, *Topics in Galois theory*, Research Notes in Mathematics, Vol. 1, Lecture notes prepared by Henri Damon With a foreword by Darmon and the author, 1992.

[9] Silverman, Joseph H., *Integer points on curves of genus* 1, J. London Math. Soc. (2), **28 (1)** (1983), 1–7.


Department of Mathematical Sciences, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon, 34141, South Korea

*E-mail address*: bhim@kaist.ac.kr

Department of Mathematics, University of Connecticut, 341 Mansfield Road U1009, Storrs, Connecticut 06269-1009, United States
*E-mail address*: erik.wallace@uconn.edu